AMENDMENTS

Please amend the present application as follows:

Claims

The following is a copy of Applicants' claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("——"), as is applicable:

1-54. (Canceled)

55. (Previously presented) A method for securely storing encrypted programming received at a receiver in a subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving a first ciphertext packet having multiple layers of encryption thereon at the receiver; and

applying a cryptographic algorithm to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

56. (Original) The method of claim 55, wherein the second ciphertext packet corresponds to a cleartext packet that was encrypted using a second cryptographic algorithm.

57. (Original) The method of claim 56, wherein the second cryptographic algorithm is a 3DES cryptographic algorithm.

58. (Original) The method of claim 55, wherein the multiple layers of an encryption include a first layer and a second layer.

59. (Original) The method of claim 58, wherein the first layer of encryption corresponds to applying a second cryptographic algorithm to convert a cleartext packet to a third ciphertext packet.

60. (Original) The method of claim 59, wherein the second cryptographic algorithm is a DES algorithm.

61. (Original) The method of claim 59, wherein the second layer of encryption corresponds to applying a third cryptographic algorithm to convert the third ciphertext packet to the first ciphertext packet.

62. (Original) The method of claim 61, wherein the third cryptographic algorithm is a DES algorithm.

63. (Original) The method of claim 55, further including the steps of:

applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a cleartext packet.

64. (Original) The method of claim 63, wherein the second cryptographic algorithm is a 3DES algorithm.

65. (Original) The method of claim 63, further including the step of:

converting the cleartext packet from a first format to a second format.

66. (Original) The method of claim 65, wherein the first format is an MPEG format.

67. (Original) The method of claim 55, further including the step of:

receiving multiple keys, each key associated with at least one layer of encryption of the first ciphertext packet.

68. (Original) The method of claim 55, further including the step of:

generating a key for use with the cryptographic algorithm.

69. (Previously presented) A method for providing a subscriber of a subscriber network with a program, the subscriber network including a headend with a plurality of receivers coupled thereto, at the headend the method comprising the steps of:

receiving a first ciphertext packet;

applying a cryptographic algorithm with a key to the first ciphertext packet to convert the first ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received at the headend to a cleartext packet;

transmitting the second ciphertext packet; and

at the receiver the method comprising the steps of:

receiving the second ciphertext packet having multiple layers of encryption thereon; and

applying a second cryptographic algorithm to the second ciphertext packet to convert the second ciphertext packet to a third ciphertext packet without first converting the second ciphertext packet to a cleartext packet.

70. (Original) The method of claim 69, wherein the first ciphertext packet corresponds to a cleartext packet that was encrypted by a third cryptographic algorithm using a second key.

71. (Original) The method of claim 70, wherein the first, the second and the third cryptographic algorithms are the same.

72. (Original) The method of claim 71, wherein the first cryptographic algorithm is a DES algorithm.

73. (Original) The method of claim 69, wherein the third ciphertext packet corresponds to a cleartext packet that was encrypted using a forth cryptographic algorithm.

74. (Original) The method of claim 73, wherein the fourth cryptographic algorithm is a 3DES cryptographic algorithm.

75. (Original) The method of claim 69, at the receiver, further including the step of:

applying a third cryptographic algorithm to the third ciphertext packet to convert the third ciphertext packet to a cleartext packet.

76. (Original) The method of claim 75, wherein the third cryptographic algorithm is a 3DES algorithm.

77-82. (Canceled)

83. (Previously presented) A receiver in a subscriber network that receives encrypted programming from a headend of the subscriber network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

a port adapted to receive a first ciphertext packet of the encrypted programming, the first ciphertext packet corresponding to a cleartext packet having multiple layers of encryption thereon;

a key generator adapted to generate an encryption key; and

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to apply a cryptographic algorithm using the encryption key to the first ciphertext packet to convert the ciphertext packet to a second ciphertext packet without first converting the first ciphertext packet received from the headend to a cleartext packet.

84. (Original) The receiver of claim 83, further including:

a storage device in communication with the cryptographic device, the storage device adapted to store the second ciphertext packet and the encryption key.

85. (Original) The receiver of claim 83, further including:

an output port in communication with the cryptographic device, the output port adapted to interface with external storage devices.

86. (Original) The receiver of claim 83, wherein the cryptographic algorithm is a DES algorithm.

87. (Original) The receiver of claim 83, wherein the second ciphertext packet corresponds to a cleartext packet encrypted by a 3DES algorithm.

88. (Original) The receiver of claim 83, wherein the input port is adapted to receive at least one decryption key, and the cryptographic device is adapted to use the at least one decryption key with the encryption key and a second cryptographic algorithm to convert the second ciphertext packet to the corresponding cleartext packet.

89. (Original) The receiver of claim 88, wherein the second cryptographic algorithm is a 3DES algorithm.

90. (Original) The receiver of claim 88, further including:

a converter adapted to convert the cleartext packet from a first format to a second format.

91. (Original) The receiver of claim 90, wherein the first format is an MPEG format.

92-104. (Canceled)

105. (Previously presented) A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key, a second key and a third key, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, the second key and the third key;

generating a fourth key;

applying to the first ciphertext packet a second cryptographic algorithm with the first key to convert the first ciphertext packet to a second ciphertext packet having two layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet; and

applying to the second ciphertext packet a third cryptographic algorithm with the fourth key to convert the second ciphertext packet to a third ciphertext packet having a third layer of encryption thereon without first converting the second ciphertext packet to a cleartext packet.

106. (Original) The method of claim 105, wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of:

storing the third ciphertext packet and the second, third and fourth keys at the subscriber location.

107. (Original) The method of claim 106, further including the steps of:

retrieving the third ciphertext packet and the second, third and fourth keys from storage; and

decrypting the third ciphertext packet by applying a fourth cryptographic algorithm to third ciphertext packet with the second, third and fourth keys, thereby converting the third ciphertext packet to a cleartext packet.

108. (Original) The method of claim 107, further including the step of:

converting the cleartext packet from a first format to a second format.

109. (Original) The method of claim 108, wherein the first format is an MPEG format.

110. (Previously presented) A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key;

a key generator adapted to generate a fourth key;

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a second cryptographic algorithm and the first key without first converting the first ciphertext packet received from the headend to a cleartext packet and thereafter to convert the second ciphertext packet to a third ciphertext packet using a third cryptographic algorithm and the fourth key without first converting the second ciphertext packet to a cleartext packet; and

a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys.

111. (Original) The receiver of claim 110, wherein the cryptographic device is further adapted to decrypt the third ciphertext packet by applying a fourth cryptographic algorithm to the third ciphertext packet with the second, third and fourth keys thereby converting the third ciphertext packet to a cleartext packet.

112. (Original) The receiver of claim 111, wherein the first, second and third cryptographic algorithms are a DES algorithm and the fourth cryptographic algorithm is a 3DES algorithm.

113. (Original) The receiver of claim 111, further including:

a converter in communication with the cryptographic device adapted to convert the cleartext packet from a first format to a second format.

114. (Original) The receiver of claim 113, wherein the first format is an MPEG format.

115. (Previously presented) A method for securely storing encrypted programming received at a receiver in a subscriber television network, wherein the encrypted programming includes a plurality of ciphertext packets, the method comprising the steps of:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver and a first key and a second key, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;

generating a third key; and

applying to the first ciphertext packet a third cryptographic algorithm with the third key to convert the first ciphertext packet to a second ciphertext packet having three layers of encryption thereon without first converting the first ciphertext packet received from the headend to a cleartext packet.

116. (Original) The method of claim 115, wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of:

storing the third ciphertext packet and the first, second and third keys at the subscriber location.

117. (Original) The method of claim 116, further including the steps of:

retrieving the third ciphertext packet and the first, second and third keys from storage; and

decrypting the third ciphertext packet by applying a fourth cryptographic algorithm to third ciphertext packet with the first, second and third keys, thereby converting the third ciphertext packet to a cleartext packet.

118. (Original) The method of claim 117, further including the step of:

converting the cleartext packet from a first format to a second format.

119. (Original) The method of claim 118, wherein the first format is an MPEG format.

120. (Previously presented) A receiver in a subscriber cable television network that receives encrypted programming, from a headend of the subscriber cable television network, wherein the encrypted programming includes a plurality of ciphertext packets, the receiver comprising:

an input port adapted to receive a first key and a second key and a first ciphertext of the encrypted programming, wherein the first ciphertext packet has two layers of encryption thereon that were applied by a first cryptographic algorithm using the first key and a second cryptographic algorithm using the second key;

a key generator adapted to generate a third key;

a cryptographic device in communication with the input port and the key generator, the cryptographic device adapted to convert the first ciphertext packet to a second ciphertext packet using a third cryptographic algorithm and the third key without first converting the first ciphertext packet received from the headend to a cleartext packet; and

a storage device in communication with the cryptographic device adapted to store the second ciphertext packet and the first, second and third keys.

121. (Original) The receiver of claim 120, wherein the cryptographic device is further adapted to decrypt the third ciphertext packet by applying a fourth cryptographic algorithm to the third ciphertext packet with the first, second and third keys thereby converting the third ciphertext packet to a cleartext packet.

122. (Original) The receiver of claim 121, wherein the first, second and third cryptographic algorithms are a DES algorithm and the fourth cryptographic algorithm is a 3DES algorithm.

123. (Original) The receiver of claim 121, further including:

a converter in communication with the cryptographic device adapted to convert the cleartext packet from a first format to a second format.

124. (Original) The receiver of claim 123, wherein the first format is an MPEG format.